Características das Cidades Inteligentes e da Internet das Coisas

Laercio Cruvinel Júnior

Departamento de Sistemas e Informática

Conteúdo

1. Introdução 3
2. Características Tecnológicas da Internet das Coisas 3
3. Redes de Sensores Sem Fio (*Wireless Sensor Networks* ou WSN) 4
4. O desafio de segurança da Internet das Coisas 5
Referências 6

1. Introdução

Vamos examinar o que se entende pelos termos Cidades Inteligentes (*Smart Cities* em Inglês), Internet das Coisas (*Internet of Things*, abreviado IoT) e qual a relação entre eles.

Cidades Inteligentes são aquelas que aproveitam a infraestrutura de comunicações e Internet para a gestão urbana com preocupações ambientais e de sustentabilidade, mas também para prover (ou melhorar) uma série de serviços de comodidade aos seus cidadãos e aos negócios residentes. Por exemplo, informações facilitadoras para o trânsito, condições do ar, gastos e poupanças energéticas instantâneas na cidade, etc.

A Internet das Coisas é a coletividade dos grupos de dispositivos e equipamentos que interagem computacionalmente com um objetivo global. Por exemplo, vários geradores eólicos podem "conversar" uns com os outros e também com a rede elétrica para otimizar a entrega de energia. Além disso, esses dispositivos oferecem interfaces de gestão remota e podem disponibilizar alguma informação publicamente. Na prática, os agentes de monitoramento chamam-se SENSORES. Por outro lado, os ATUADORES podem alterar as condições operacionais do equipamento monitorado, segundo uma programação prévia em resposta a dados dos sensores ou como resultado de comandos de gestão. Assim, pode existir um grau de inteligência e adaptabilidade nos grupos de dispositivos e equipamentos da Internet das Coisas. As redes de comunicação permitem que os grupos integrem-se também uns com os outros para diversos propósitos.

A Internet das Coisas é habilitadora das Cidades Inteligentes, fornecendo a base tecnológica para a melhoria dos serviços existentes e o desenvolvimento de novos serviços para os cidadãos. Por exemplo, melhorar o tráfego através de sensores nas estruturas urbanas e nos veículos que monitorem os padrões de tráfego (imaginem um Waze mais abrangente e confiável). O consumo de energia de prédios e casas também pode ser melhor monitorado e otimizado automaticamente. Os *smartphones* são indiscutivelmente parte integrante da IoT e podem ampliar a rede de sensores, ao mesmo tempo que permitem ao cidadão usufruir dos serviços disponibilizados pela edilidade e participar ativamente na governança da sua cidade.

2. Características Tecnológicas da Internet das Coisas

Vimos que a Internet das Coisas, ou IoT em inglês, é fundamental para o conceito de Cidades Inteligentes, porque é através da IoT que pode ser feito o monitoramento e ajuste de condições operacionais dos diversos serviços urbanos.

Para um centro urbano médio, e excluídos os diversos mecanismos inerentes aos cidadãos (*smartphones* e outros equipamentos com acesso a redes, tais como Google Glasses), projeta-se a necessidade de milhares, talvez dezenas de milhares de equipamentos sensores, necessariamente pequenos mas com alguma inteligência. Um sensor típico tem alguma capacidade de processamento, um pouco de memória, um sistema operacional especializado e capacidade de comunicação com outros sensores ou com alguma estação central. Tudo isso, mais a infraestrutura de comunicação, custa dinheiro e estima-se que a viabilidade da Cidade Inteligente passe por sensores com preço médio de 5 euros e baixíssimo consumo de energia.

Outro aspecto a levar em conta na implantação de sensores em zonas urbanas é a segurança do sistema. É necessário dificultar que os sensores sejam "hackeados" ou danificados fisicamente. A primeira ameaça pode ser combatida com métodos sofisticados de encriptação (mas que exigem mais capacidade de processamento e possivelmente mais memória individualmente), e o acesso físico pode ser dificultado pela incorporação dos sensores em equipamentos urbanos mais corriqueiros (como postes de iluminação, etc.).

Um pouco mais a jusante, no centro de controlo desses sensores, será necessária capacidade de processamento e comunicação de dados capaz de receber e enviar informação para as dezenas de milhares de sensores e atuadores. A informação que recebe nem sempre tem de ser em tempo real, mas a quantidade de dados obriga a aproximações tipo Big Data e Mineração de Dados (tecnologias capazes de gerar informação útil a partir de muito grandes quantidades de dados em bruto), para que as respostas possam ser consistentes com a expectativa dos cidadãos usuários dos serviços e com as necessidades de gestão do centro urbano. Estas necessidades também serão provavelmente diferenciadas conforme o horário e dia.

3. Redes de Sensores Sem Fio (*Wireless Sensor Networks* ou WSN)

Vimos acima que a Internet das Coisas inicia no agrupamento de dispositivos sensores, que podem transmitir informação sobre o ambiente (temperatura, luz, proximidade, calor, dióxido de carbono, humidade do solo, aplicações de vigilância eletrônica, etc.) e que podem ser remotamente configurados e administrados.

Os dispositivos de um destes grupos muitas vezes não estarão fisicamente conectados uns aos outros, formando então uma rede sem fios (*wireless*), daí o nome WSN ou Rede de Sensores Sem Fio.

As vantagens dos dispositivos sem fio incluem a sua mobilidade, fácil instalação e menor custo total da solução. Desde o início do século XXI, a miniaturização dos componentes tem andado a par com baixa de preço e integração (muitas vezes os diversos componentes de um dispositivo sensor são completamente integrados em um só *chip*). A comunicação sem necessidade de usar cabos físicos viabiliza uma grande gama de soluções com sensores, tais como os sensores em automóveis ou em animais, ou mesmo embebidos no corpo humano e relatando diversas condições de saúde ou servindo de tornozeleira eletrônica para controlar criminosos.

Uma tecnologia de integração para dispositivos sensores e atuadores com notável evolução recente são os sistemas micro-eletro-mecânicos (a sigla em inglês é MEMS). Esta tecnologia permite fabricar sensores e atuadores com tamanhos milimétricos ou menores). Sensores fabricados com esta tecnologia geralmente usam como fonte de energia o próprio meio em que se encontram, transformando luz, vibração ou calor na eletricidade necessária para o seu funcionamento.

Tal como aconteceria se os sensores estivessem em uma rede cabeada, o propósito de uma rede de sensores sem fio é permitir a cooperação entre os diversos dispositivos na monitoração e possivelmente no controle do ambiente. Essa colaboração não impede o

funcionamento autônomo de cada dispositivo, por exemplo para escolher a melhor rota (o melhor vizinho) quando deve enviar dados. Assim, essas redes são definidas no momento em que forem ser utilizadas - diz-se que são redes *ad hoc*, um termo do latim que significa "com esta finalidade". Assim, uma WSN é auto-organizável e dinamicamente estruturada e muda as rotas de envios de dados e comandos sempre que é adicionado ou retirado um dispositivo, ou quando um dispositivo se move, ou quando muda alguma condição ambiental que interfere na comunicação entre dispositivos.

Um dos dispositivos na WSN é uma porta (*gateway*) para a Internet, ou para uma rede privada ou de operador telefónico, permitindo a comunicação com o centro de dados ou estação de controlo onde os dados são armazenados e de onde são emitidos os comandos de configuração e atuação para os dispositivos da WSN. Por questões de desempenho e de preservação de energia, muitas vezes os dados são "agregados" na WSD à medida que passam pelos dispositivos até chegarem ao *gateway*, e vão agregados para a estação de controlo. O lado negativo desta aproximação é que as eventuais perdas de dados ficam mais graves (é pior perder um agregado dos dados de vários sensores do que os dados de um só sensor).

4. O desafio de segurança da Internet das Coisas

Tal como a lei da ação e reação, sempre que há um novo sistema de computação ativo na Internet, há também quem o queira "hackear": acessar remotamente e manipular, por diversão ou com fins criminosos. A proteção contra ciberataques é um dos maiores desafios quando o número de dispositivos conectados é muito elevado, como se espera que aconteça na Internet das Coisas. Porém, a atual "corrida do ouro" para lançar dispositivos conectáveis para a Internet das Coisas faz com que os fabricantes estejam mais focados em obter vantagem competitiva em funcionalidade do que em segurança.

Uma preocupação especialmente relevante é a exposição indevida de dados privados e outra informação sensível, de indivíduos ou empresas. E falamos aqui não só de equipamento público (semáforos, diversos sensores das Cidades Inteligentes) ou de telefones celulares, mas de todo o equipamento futuramente conectado: televisores, frigoríficos, monitores de animais e crianças, equipamento médico, câmeras de vigilância, rádio do carro, e outros...

Mesmo sem considerar o acesso indevido, há uma preocupação com a grande quantidade de informação (a princípio privada) que é colocada voluntariamente à disposição de corporações quando a Internet das Coisas entra em nossas casas. Em todos os cômodos de uma casa haverá possivelmente dispositivos capazes de sentir nossa presença, e registrar ações e conversas. Para efeitos de marketing dirigido, dizem as corporações...

Uma abordagem para buscar soluções passa por compreender que a arquitetura geral da Internet das Coisas pode ser modelada como um conjunto de blocos, por exemplo: a infraestrutura de rede, a infraestrutura na nuvem, os dispositivos principais de conexão entre redes, e todos os outros dispositivos, ou "coisas". Cada um desses blocos tem áreas de vulnerabilidade particulares e necessita de tecnologias específicas de *hardware* e *software* para amenizar ou resolver o problema de segurança.

Finalizamos lembrando que a Internet das Coisas tem uma arquitetura naturalmente distribuída sobre um modelo de comunicação *peer-to-peer* (cada dispositivo descobre a rede em que está através da comunicação com seus vizinhos, e passa e recebe informação através deles). Este modelo distribuído adapta-se bem a tecnologias que pretendem usar a Internet das Coisas, tal como o conceito emergente de *blockchain*, uma tecnologia que permite registrar transações distribuídas ou qualquer interação feita digitalmente, de uma forma segura e eficiente. Embora o uso mais visível de *blockchain* sejam as moedas digitais, há estudo de aplicações em outras áreas, tais como uma democracia digital (em estudo) e um modelo de governança para serviços distribuídos (já com material desenvolvido).

Referências

[IEEE Xplore] *Readings on Smart Cities*, Dezembro 2014

[IEEE Internet of Things] *Towards a Definition of the Internet of Things (IoT)*, Maio de 2015

[IEEE Internet of Things] *IEEE Talks IoT*, acedido em Março de 2017

Gartner [Internet of Things] - *Top 10 IoT Technologies for 2017 and 2018* (Webinar), publicado em 2017

IEC - International Electrotechnical Commission: *Internet of Things: Wireless Sensor Networks* (white paper), online http://www.iec.ch/whitepaper

IEEE Transmitter: *The Challenges Facing IoT*, online em http://transmitter.ieee.org

Ahmed Banafa in IEEE Internet of Things: *Three Major Challenges Facing IoT*, online em http://iot.ieee.org/newsletter/march-2017

Ahmed Banafa in IEEE Internet of Things: *IoT and Blockchain Convergence: Benefits and Challenges*, online http://iot.ieee.org/newsletter/january-2017

Jeremy Epstein in *Venture Beat, Companies of the future: No CEO, no boss, managed by blockchain*, online https://venturebeat.com/2017/04/23

Luis Fernando Molina, *Fermat Distributed Governance Model*, online https://medium.com/@luisfernandomolina